Afful Ekow Kelly, Department of Information Technology, School of Science and Engineering, Malaysia University of Science and Technology. Selangor, Malaysia.
ORCID: 0000-0002-8026-6436.
Sellappan Palaniappan, Professor, Dr., Head of Department, Department of Information Technology, School of Science and Engineering, Malaysia University of Science and Technology. Selangor, Malaysia. ORCID: 0000-0002-7650-8404.

A proposed approach to enhance user PIN in the mobile money ecosystem in Ghana

Abstract: The use of only numeric numbers as the base for the USSD PIN rather than alphanumeric was one of the security risks in the USSD mobile money services. The study objective is to assess the security threats posed by user PINs in the mobile money banking ecosystem and to enhance the service quality of the existing mobile money service with its high level of security threats prone to the mobile money industry. The study aims to shed light on the consumer acceptability requirements for mobile banking in particular areas of the consumer usage pattern, which will inform the industry players to strengthen such areas in consumer interest. This will help both the telecoms to understand the individuals and customise services based on the service needs of users of their product. This will aid the operators to cut costs and help improve the security infrastructure in other countries to cover to rope in more users, and to serve the unbanked in the hinterlands of the country. There is a growing demand for the adoption of mobile money services in Ghana. However, there is insufficient research to understand the risk associated with the adoption of the service. It is on this trend that, the study sought to reveal and understand the threat in the nature of user PIN used in the mobile money service. This study encapsulates, with the extension on demographic scope, which included workers, students, employed and unemployed who have adopted mobile money services the study adopted an exploratory method, to understand the main threats of the user PIN in relation to the mobile money application adopted in Ghana. This also included a survey question for users' responses on the nature of use. The study included 57 participants to uncover the vulnerability of users' PINs in mobile money services. The study's findings revealed that the length could be increased. The current size of the PIN stack was set to four for convenience and user-friendliness, with little thought given to the threat such a length could pose in financial transactions involving mobile money banking. The mobile money PIN solution provided will enable users not to be worried n about their accounts should users end up losing their handset and otherwise potentially harm their handsets because the merchandise is completely secure. The system is safeguarded by cutting-edge secure authentication, but also users' funds are always secure because each transaction requires a secured alphanumeric password. The mobile payment process delivers individual clients with enhanced security but also lowers the need of carrying physical money but also ensures easy prompt payment of transactions of utilities. Individuals utilizing such services will manage to pay one's bill payments from the comfort of their place of arbour and making it even easier to do so. The use of only a numeric key for PIN was far more convenient for users, but it also made them more vulnerable to attacks. The standard PIN length in the current USSD mobile money application was four numeric keys. The indication was that the PIN length was too simple for a simple system to break through. The study proposed solution where mobile

money users can increase their user PIN to six characters, and include alphanumeric keys. The study will help reduce the increasing threat of mobile money fraud in the FinTech industry.

Introduction

Ghana's mobile telecommunications industry (GMTI) is among the most competitive sectors in Africa, considering massive foreign actors in the telecoms industries (*Yeboah-Asiamah et al., 2016*; *De Luna et al., 2019*) and has also been generally viewed as the most influential aspect of Ghana's economy. Mobile telephone subscribers stood at 41 million at the end of 2021, depicting a 134 percent penetration rate in 2021, National Communication Authority – NCA (*National Communication Authority, 2021*). The emergence of mobile money has altered how businesses are conducted (*Madise, 2019*; *Jakhiya et al., 2020*). Customers are required to register with users' national identity card (Ghana card) to any selected telecoms across the country. The user's SIM is automatically registered for mobile money service when a user signs up, which is mandated by NCA for network operators (*Act, 769*). Users need not open a bank account before using the mobile money application because mobile applications do not require a bank account to function.

There is sufficient research on mobile money and mobile banking, in the areas of stakeholders' perspective (*Mullan et al., 2017*) individual performance (*Munoz-Leiva et al, 2017*) service quality (*Kaatz, 2020*; *Desmal et al, 2019*), security (*Wazid et al., 2019*; *Otor et al., 2020*), and as a financial tool in an emerging economy (*Malaquias & Silva, 2020*; *Tripathi, 2020*; *Mohamed & Nor, 2021*), indicate the impact on the financial growth it has brought to those countries, and most importantly the users of the mobile money banking service. Mobile money is challenged with fraudulent activities, thus the focus of the study, is the length of user PIN used in the mobile money service.

The direct interaction between the telecoms and handset is by use of a web portal and short message service (SMS), where SMS is through unstructured supplementary service data (USSD) however, the SMS is the most common medium (*Mallik et al., 2020*). SMS usage has grown in almost every sector of human development, from health care, e-government, education, agriculture, railways, mobile banking, and news alert to send reminders. These messages also include passwords and private information of users in 2018 (*Shital and Prakash, 2015*), more than 9.1 trillion SMS were sent across the globe, constituting 1 trillion dollars US in commercial value.

Mobile technology has successfully revealed itself as a digital platform for various activities, including online banking and mobile money services (*Khan et al., 2017*; *Lin et al., 2020*). While designing mobile applications, there are a few other issues to solve, including simplicity of the application, user friendly, security, and a well-established application referred to as a "killer application" (*Siau et al., 2003*). According to S. Hillman and C. Neustaedter (*Hillman & Neustaedter, 2017*), mobile application development is simply by virtue of whether such regulatory approval potentially makes service providers more reliable with their mobile application services (*Munoz-Leiva et al, 2017*; *Jagtiani & John, 2018*; *Bowers et al., 2017*; *Chen, 2019*). Transfer funds on

the mobile application is more than yet another software on one's phone, but rather an embodiment of the institution's brand. However, according to S. Sarkar and A. Khare (*Sarkar & Khare, 2019*), users would be discouraged from establishing flaws in the applications they are using, as a result, mobile device architects must thoroughly examine the applications environment.

The usefulness of the mobile handset is becoming tough with various mobile devices, which have decreased in size and weight over time (*Venkatesh et al., 2012*). Moreover, the conventional mobile applications' adaptability is still unsolved since the applications should be able to adjust to users' requirements and requests and ensure their mobility (*Anagnostopoulou et al., 2017*; *Wang et al., 2018*). Developing the technical support provided by information technology infrastructure is the primary difficulty in mobile apps and the user's ability to operate a smartphone application. On the other hand, the advent of numerous traditional financial misfortunes has highlighted the difficulties inherent in the mobile money system, which is used throughout the mobile payment transaction process (*Mega, 2020*; *Lee et al., 2018*).

A suitable system of payments through mobile devices is also a challenge in the evolution of mobile banking (*De Luna, 2019*; *Kim et al., 2020*; *Wang et al., 2021*), as mobile devices function as a strong medium in financial solutions also including mobile payments and mobile money services. Therefore, designing mobile money applications thoroughly to satisfy the needs of target users is highly significant (*Korableva et al., 2019*; *Ahmad et al., 2018*).

The use of mobile money has become very important in bridging the most critical services that also occurred during the Covid-19 pandemic (*Bryant et al., 2020*; *Beaunoyer et al., 2020*). The role of mobile money became a saviour in the financial sector during the covid-19 pandemic. The use of mobile money allows users to transfer money to anybody who also had a mobile device and is registered with any mobile money company. Those whose SIM is not registered to any mobile money service operator were allowed to use the token option, the mobile money banking services give room to users to settle bills, purchase prepaid airtime, check their bank balance, and buy products and services using the service (*Jakhiya et al., 2020*; *Gosavi, 2018*).

Research Problem

There is an adequate study on mobile money and mobile banking, including stakeholders, service quality, security and financial tool for an emerging economy (*Munoz-Leiva et al., 2017*; *Desmal et al., 2019*; *Otor et al., 2020*; *Malaquias & Silva, 2020*; *Tripathi, 2020*). These studies show the impact mobile money had on financial growth in those countries where it has been adopted, and most importantly, the mobile money service users. However, there is little scientific and empirical evidence as to what has led to the security threat related to mobile money services in Ghana.

The importance of the usage of USSD for mobile money should not elude stakeholders from overlooking the emerging security threats associated with mobile money services. It is on this score that the study is to highlight the weakness of the current user PIN used in the mobile money service and introduces an increased PIN length instead of the four numeric PINs currently used.

The threat to mobile money has become obvious, and fraudsters have taken advantage to wreak even more havoc on users, while service providers appear to do nothing to address the

obvious issues, instead simply asking users to be cautious with how they handle their PIN. Third-party access to a user's PIN has become a common method for fraudsters to gain control of a user's account. However, there is no guarantee to protect users regarding how their accounts are operated, nor are there any security measures in place to ensure some level of safety on their accounts.

As a result, the study problem is to improve the user's security PIN of mobile money services and the threats that characterise the mobile money industry.

Literature

The review considers the structures associated with mobile money applications, as well as the security risk posed by USSD structures linked to mobile money services.

Mobile application issues

The problems of accepting mobile money have been widely studied and referenced based on one's geographical location and class of development associated with mobile money services (*Khalilzadeh et al., 2017*). There is a litany of challenges confronting the mobile money payment system. The challenges discussed by researchers are tailored toward the scope of their study and the purpose set for the study. The study, therefore, classified the challenges confronting mobile payment as; security, cost, standardisation, convenience and technology, and system quality (*Kang, 2018*). The fundamental taste of users to adopt technology varies. However, T. Dahlberg and N. Mallat indicate that the focus should be on safety and affordability to get customers to embrace the new payment system (*Dahlberg & Mallat, 2002*). The study considers in detail the challenges relating to the acceptance of mobile payment systems. Figure 1 summarises the challenges in mobile money applications, and any solutions proposed must attempt to address them (*Figure 1*).

Standardisation

Several academics suggest that the unavailability of a uniform approach poses apparent issues in the advancement of mobile payment services to attract users (*Verkijika & Neneh, 2021*). According to MeT, the usage of mobile banking current market is characteristic of either an emerging thing, first with a plethora of concepts and indeed ideas, which might or might not be interoperable (*MeT, 2001*). Also, with a standard interface since the shared knowledge and convenience of use are vital, all the customers' delight is getting a service that meets their requirements and service deployment at ease. Finally, one of the most pressing issues in mobile payments is a lack of standardisation, exacerbated by the mobile market's proliferation (*Hillman & Neustaedter, 2017*; *Yan, 2021*).

Trust

Trust in mobile payment services is mostly limited to devices, applications, operators, regulations, and network infrastructure (*Yeboah-Asiamah et al., 2016*; *Baganzi & Lau, 2017*). Trust encapsulates the fact that the user strongly expects that the data and transaction information that the operators and the banks primarily handle are not misused or trade-off but is kept safe (*Sharma*

& Sharma, 2019; Talwar et al., 2020). This could be done when all the players put in appropriate measures to ensure and assume the trust needed.

System quality

Consumers obtain good impressions and adoption when they see that the service offers to them is of good quality (Zhu et al., 2017). The strength of third-party trustees, the crucial cryptography infrastructure to check secure transactions and the safeguard of privacy is an unquestionably crucial aspects in creating consumer adoption.

According to B.J. Corbitt and Y.T. Han, when customers find inadequate integrity, it may hinder their interest to use (Corbitt & Han, 2003). However, system quality should primarily put into perspective the user's demand to understand how it will ease their response to service demand.

Convenience

Convenience and ease of use are both significant factors incentivising all technological advancements (Jibril et al., 2020; Pal et al., 2020). Mobile user views of mobile payment convenience have a favourable impact on the acceptance of "mobile payment services" (Humbani & Wiese, 2018). Consequently, the accessibility of mobile payment systems is one of the reasons behind their popularity. However, in this age of rising hacking and cyber fraud, mobile money transactions come with the risk of financial and data loss. Compared to traditional financial service providers, the perceived benefit of the desire to use mobile payment is an appropriate basis to attribute the perceived usefulness of the intention to adopt mobile financial services (Putritama, 2019). According to W. Liu, X. Wang, and W. Peng, although mobile payment is convenient, it also introduces dozens of new payment security concerns, leading to our subsequent discussion on security (Liu et al., 2020).

Security

Security knowledge, privacy issues, and trust problems are all possible causes of factors to disrupt the gains made in mobile commerce (Otor et al., 2020; Kang, 2018). Thus "mobile commerce started with the establishment of cellphones equipped with advanced cards" (Madden et al., 2017), which provide security features not accessible through all the other e-commerce methods. The cell phone, with an embedded SIM card, is an ideal recipient for a public key infrastructure (PKI) system's secret key electronic signature (Prakasha et al., 2019).

However, this advancement is only possible if a tremendous amount of data security is ensured for the user's information and secured transactions (Arun Prakash et al., 2018; Feng et al., 2017). According to F. Gao, P.L.P. Rau, and Y. Zhang, the rising "adoption of mobile devices, as well as the development of digital systems" and applications, necessitates a human-centred approach to mobile data security (Gao et al., 2018). Privacy is a fundamental consumer prerogative, as users must not divulge their identity to other parties unless they are ready to provide that privilege (Bowers et al., 2017).

Cost

Another factor that keeps surfacing in the face of adopting mobile payment is the transaction cost associated with the services provided, and related charges have not been easy. This is supported by (*Abooleet & Fang, 2021*), according to them, most of these payment methods continue to face opposition due to a variety of factors, such as transaction costs. The acceptability of mobile money payment is completely dependent on those willing to pay the extra cost (*Liu et al., 2019*; *Shaw & Sergueeva, 2019*). It is, of course, not simple to convince clients to give more charges without good offerings. Operational expenses include both fixed but also payment system expenses, as well as user expenditures and technological infrastructure.

Cost, security, convenience, system quality, standardisation and trust are major factors for application development package standards for developers and users. The application issues associated with the development of mobile money services are the yardstick for developers and users in determining the application quality. These measures aid the success and failure in the acceptance of mobile money applications and services.

Security threats in SMS

Information security is the act of protecting information systems from unauthorised access for use any other than its original purpose. The distribution of SMS via a GSM system is not secured and is vulnerable to unauthorised access (*Donald & Favour, 2021*).

Common threats in SMS

The nature of the attack in a network system can be placed into two forms, thus internal and external; which could also be referred to as active and passive respectively (*Sudin et al., 2018*; *Ghannam et al., 2018*). We look closely at the specific attacks related to networks from which SMS is predominant in mobile money transactions. Figure 2, shows some SMS threats, these threats have become a challenge to most mobile money services (*Figure 2*).

1. Man-in-middle Attack: this happens when the user is falsely authenticated by the use of a false network system. Before any message or call gets through, the user has to be verified; this is where the attack happens, the man-in-middle turn to use a "false base transceiver station which uses the same network code of the subscriber", which makes it difficult to notice of the false authentication, as a result, turns to impersonate or commit any crime on the network.

2. Replay Attack: with a replay attack, the perpetrator uses the old messages between the user and the network to carry out such attacks. The user turns to trust the source and is ready to do anything such inquest this new message seeks to achieve.

3. Spamming: these are SMS messages which are sent as a nuisance or for an attack such as phishing or pharming. Several social marketers online turn to using SMS messages as a very legitimate marketing tool. But these turn out to be an inconvenience in some cases.

4. Denial of Service (DoS) Attacks: this happens when bulk and repeated SMS messages are sent to a target mobile phone user, with the primary intention to deny the user the use of their phone.

5. SMS Phishing: this uses the weakness in the SMS to send unsolicited information to a user with the main intention to cause harm.

6. Message Disclosure: SMS by default is not encrypted; the user's message is temporarily stored in SMSC as plain text. This makes the SMSC Centre venerable to an attack, as such messages are intercepted either deliberately or by a brute force attack. The information gotten could be used for a purpose which is not intended by the user. In some instances, the information could be of no use but viewed by a third party.

Figure 2 depicts the SMS threat associated with the USSD application in mobile money services (*Figure 2*).

Research Methodology

Research methodology is a system of methods used scientifically to solve the study problem. According to J.W. Creswell and J.D. Creswell, research must have a general framework; which aids in the design, structure and research strategy (*Creswell & Creswell, 2018*). The framework considered for this study is the research design and the data collection method and analysis to be used.

According to J.W. Creswell and J.D. Creswell, research designs are strategies and procedures spanning from presumptions to precise methods of data collection, process, and interpretation (*Creswell & Creswell, 2018*). The study adopted an exploratory design, thus exploratory sequential. This method first considered a qualitative aspect of the study then followed by a quantitative with the major aid in developing an intervention or designing an application to support the study (*Glyptis et al., 2020*).

The study first had a panel discussion with experts in the mobile money banking industry; these included professionals who had once worked with the mobile banking industry and the Telecoms. Moreover, the study team met the mobile money operators and agents in their capacity and not the institution. The reason for not meeting any of the telecoms officials was, they did not respond to the several letters requesting a meeting to have an overview understanding of the kind of security operations adopted by the telecoms in the mobile money service.

The study organised a focus group discussion and engaged a group of mobile money users through a purposive survey method to give insight into the PIN composition for mobile money services. The survey to get insight into users' PIN patterns was one of the most strenuous aspects of the study since most users were never willing to take part in the study. The outlook from the survey shows the kind of PIN users create. This revealed the weakness of the user PIN and how easily a third party through social engineering and social media can get access to the user PIN. Only 57 participants took part in the study. Table 1 shows the outcome of respondents' pattern of choosing and creating user PINs for mobile money (*Table 1*). The participants were asked to change their PIN after the survey.

The analysis of the study was to develop a mobile money application that will function just the same as the current mobile money application adopted by telecoms. The analysis adopted is to ensure that the study's mobile money application functionality solves the challenges set for the study's focus.

The scenario in Figure 3 enforces the kind of PIN used and its lengths, this is easier and simple for the user (*Figure 3*). However, it unveils how vulnerable it is to access a user's mobile money PIN (*Delahaye, 2019*).

The masking technique prevents the risk user is exposed to when using mobile money through shoulder surfing. Some users don't see the need to have a masked PIN, and most users in the study responded to the need not to mask their PIN. However, there are quite a number of research which the proposition to have a masked PIN is strong (*Agbezoutsi et al., 2021*; *Tiwari et al., 2020*). Figure 4 demonstrates the user PIN entered for a transaction; this also shows how easy it's for anyone to get hold of the user's PIN (*Figure 4*).

There are several methods used to overcome the masking of PIN. The two ways to implement the masking methods. First, there could be complete masking of the PIN, where the user is not having any option of seeing what they are typing, but the user must know precisely the PIN required for that session. Secondly, the other choice is where the user is given an option; thus, a check option allows the user to see the PIN entered. There has been advertising use and implementation of the "Mobile PIN" concept where users can set their PINs (*Tiwari et al., 2020*; *Lakshmi et al., 2017*). However, this concept does not resolve the current threat related to the application's inability to mask the input PIN from the user. Therefore, the PIN adopted and used by the user through the USSD application remains a threat. In the case of the mobile money service application used by telecoms, none of the service providers implements PIN masking. This loophole in the mobile money service application has been exploited towards the disadvantage of mobile money users. This is not subject to any mobile money service providers; none of the service providers implores any masking options discussed.

Application development tools

The service tools used for the development of the mobile money application, first, a local host server was created to expose the codes to the Internet and AfricaTalk as simulation platforms. The study adopted Apache HTTP Server as the internal server host. Also, ngrok was used to help tunnel the service of the webserver (Apache). For, the webserver and ngrok not to delay in the kind of service it is rendering a Callback is used to support the flow of data access, this serves as stationery to where the webserver and external host can easily and continuously fetch its data for their use as and when it is needed.

Proposed User Pin Solution for USSD Mobile Money Service

The number of characters used as PIN authentication generally determines the PIN's strength. Using "mobile money" services as a case, all the telecom operators' PINs are limited to only four (4) numeric characters. This makes it easier for anyone mindful of accessing another user's PIN with minimum brute force attack or shoulder looking to get hold of an individual PIN quickly (*Delahaye, 2019*). In contrast, with that comes a gap this study would want to fill in the current security arrangement by the operator of the telecom of mobile money in Ghana.

This demonstrated that the PIN length could be broken in less than an hour using simple computer algorithms in a brute-force attack (*Delahaye, 2019*). The current size of the PIN stack was set to four for convenience and user-friendliness, with little thought given to the threat such a length could pose in financial transactions involving mobile money banking. This resulted in users not making any conscious effort to create PINs that were difficult to guess. In any case, given the length of available keys, users simply used any patterns that were as convenient to them, such as the last four digits of their current phone number or their year of birth, as was

discussed earlier. As a result, the study implementation in order to increase the length of the PIN key was successful. This was increased to six characters on the basis that if a user loses or misplaces their phone, they will have a much greater window of opportunity to report it to the appropriate telecommunications operators. The latter will then block access to the phone to be used by the default new owner. As a result, it is a win-win situation for both telecoms and users.

Figure 5, illustrates the coding to increase the length to six characters from the current designated of four numbers (*Figure 5*). This introduction gives users the freedom to use any key combination of up to six characters, thus alphanumeric characters instead of only numeric ones. This is not to say that users cannot continue to use the year of birth and other patterns discussed previously. However, users can add any additional characters to their existing keys. This makes the user's PIN length longer, and it is a little more difficult to brute-force attack the user's financial account on the mobile money platform. Figure 6 shows what the mobile money interface looks when a user enters their PIN in a transaction process (*Figure 6*).

Discussion

There are some participants who use "digits of their phone numbers" from the given phone number scenario (0244 906 732) for clarity. Some users used the last four (4) digits of their phone numbers (6732); others used the first four (4) digits (4906) apart from the phone code (024, 020, 054, 055, 027). Considering the perspective of gender, most females used their last digit as a PIN compared to males, and most males used the first four digits of their phone numbers as a PIN compared to females.

There was some diversity in the category for those who used "year of birth"; (1934). Some used their year of birth as the PIN code, and some also used the year of birth of their boyfriends, girlfriend, fiancées, parents and kids. With the same consideration about gender and their choice of these patterns for PIN codes, most females prefer using the year of birth compared to males.

The final category is those who used "other forms" of key combinations as their PIN. The PINs used by this category are grouped into two, those just by instincts and others by familiarity with some numbers; this includes generic numbers such as (1234, 7777, and 4321). The comparison based on gender indicates more males prefer using this method of randomly combining numbers for PIN than females. The above analysis clearly shows that, with this information at hand, anyone who has access to others' phones can break into their mobile money accounts without any trace.

The final results show that PIN masking is still a major challenge to the mobile money service. The reason for not meeting the outcome of PIN masking is that the USSD platform used for mobile money development was also limited. As a result, there is technically little the study could do to achieve this, which greatly aided in understanding the relationship between the industry and its stakeholders. There is a need for telecoms to consider adopting this concept to improve the security of the mobile money banking service.

The issue addressed in the use of USSD in mobile money transactions was the length of PIN keys. In the current USSD mobile money application, the standard PIN length was four characters. The indication was that the PIN length was too simple to break through in an hour with a simple computer system. According to the findings, it was possible to increase the length

of the user PIN using the USSD application. However, this was never encouraged in the type of USSD application used by telecommunications companies.

Conclusion

The study objective is to assess the security threats posed by user PINs in the mobile money banking ecosystem and to enhance the service quality of the existing mobile money service with its high level of security threats prone to the mobile money industry.

The findings were based on the software development created for this study. In addition, the advancement was based on the exploration and quantitative study during the literature review period. These were focused on PIN length.

The simulation determination of increasing the length of the key used as a PIN for mobile money was achieved. The need and suggestion to increase the length of user PIN is to make the service more secure than what is currently used. According to Jean-Paul Delahaye, the duration of time needed to reveal the user PIN with the use of a computerised system in a brute force method is longer if the length of the key is longer (*Delahaye, 2019*). The current application key used by telecoms is four digits, this therefore clearly indicates the vulnerability associated with its use and the risk to access by fraudsters.

The outline of alphanumeric keys and the ability to increase the length of PIN in mobile money banking services will go a long way to reduce the rate of fraudulent activities on mobile money services. There is still clear evidence of a lack of collaboration between software developers and the industry in the areas of advancing the use of USSD mobile money with telecommunications companies. This was discovered by the USSD application development tool used by the telecoms for this study in the SMS sections of the USSD mobile money banking. In general, USSD was thought to be more secure than SMS in transactions (*Lakshmi et al., 2017*; *Nakibuuka et al., 2019*). Because the USSD does not keep track of the transaction histories of users. However, due to the lack of PIN masking, one major support offering the security nature of the USSD is weakened by the software development issue. According to the study reviews, masking the PIN would improve the physical security of transactions. This was done to ensure that anyone looking over their shoulder would not see the user's PIN. This singularity is still a problem for USSD mobile money banking; the platform is fixed, not allowing PIN masking.

The outcome of this study will enable decision-makers, academics and industry players to have prudent and ample reason on factors contributing to the rising numbers of threats to consumers' financial and personal data in the mobile money industry.

Acknowledgement

References:

Abooleet, S., & Fang, X. (2021). *The role of transaction cost in the adoption of mobile payment*.

Agbezoutsi, K. E., Urien, P., & Dandjinou, T. M. (2021). Mobile money traceability and federation using blockchain services. *Annals of Telecommunications*, *76*(3), 223-233.

Ahmad, A., Li, K., Feng, C., Asim, S. M., Yousif, A., & Ge, S. (2018). An empirical study of investigating mobile applications development challenges. *IEEE Access*, *6*, 17711-17728.

Anagnostopoulou, E., Magoutas, B., Bothos, E., Schrammel, J., Orji, R., & Mentzas, G. (2017, April). Exploring the links between persuasion, personality and mobility types in personalized mobility applications. In: *International conference on persuasive technology* (pp. 107-118). Springer, Cham.

Arun Prakash, R., Jayasankar, T., & VinothKumar, K. (2018). Biometric encoding and biometric authentication (BEBA) protocol for secure cloud in m-commerce environment. Appl. Math. Inf. Sci, 12(1), 255-263. https://ink.library.smu.edu.sg/sis_research/168

Baganzi, R., & Lau, A. K. (2017). Examining trust and risk in mobile money acceptance in Uganda. *Sustainability*, *9*(12), 2233.

Beaunoyer, E., Dupéré, S., & Guitton, M. J. (2020). COVID-19 and digital inequalities: Reciprocal impacts and mitigation strategies. *Computers in Human Behavior*, *111*, 106424.

Bowers, J., Reaves, B., Sherman, I. N., Traynor, P., & Butler, K. (2017). Regulators, mount up! analysis of privacy policies for mobile money services. *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 97-114.

Bryant, J., Holloway, K., Lough, O., & Willitts-King, B. (2020). Bridging humanitarian digital divides during Covid-19. HPG (ODI). https://www.odi.org/publications/17580-bridging-humanitarian-digital-divides-during-covid-19

Chen, R. (2019). Policy and Regulatory Issues with Digital Businesses. *World Bank Policy Research Working Paper*, 8948.

Corbitt, B. J., & Han, Y. T. (2003). Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications*, *2*(3), 203-215.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approach*. Sage Publications.

Dahlberg, T., & Mallat, N. (2002). Mobile payment service development: Managerial implications of consumer value perception. *Proceedings of the European Conference on Information Systems*, 649-657. Gdansk, Poland: ECIS.

De Luna, I. R., Liébana-Cabanillas, F., Sánchez-Fernández, J., & Muñoz-Leiva, F. (2019). Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied. *Technological Forecasting and Social Change*, *146*, 931-944.

Delahaye, J.-P. (2019). The mathematics of (hacking) passwords. https://www.scientificamerican.com/article/the-mathematics-of-hacking-passwords/

Desmal, A. J., Othman, M. K. B., Hamid, S. B., Zolait, A. H., & Kassim, N. B. A. (2019, August). Proposing a service quality framework for mobile commerce. *International Conference for Emerging Technologies in Computing*, 203-212. Cham: Springer.

Donald, E., & Favour, O. N. (2021). Analysing GSM Insecurity. *arXiv preprint arXiv:2109.12408*.

Feng, W., Zhou, J., Dan, C., Peiyan, Z., & Li, Z. (2017). Research on mobile commerce payment management based on the face biometric authentication. *International Journal of Mobile Communications*, *15*(3), 278-305.

Gao, F., Rau, P. L. P., & Zhang, Y. (2018). Perceived mobile information security and adoption of mobile payment services in China. *Mobile Commerce: Concepts, Methodologies, Tools, and Applications*, 1179-1198. IGI Global.

Ghannam, R., Sharevski, F., & Chung, A. (2018, October). User-targeted denial-of-service attacks in LTE mobile networks. *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 1-8. IEEE.

Glyptis, L., Christofi, M., Vrontis, D., Del Giudice, M., Dimitriou, S., & Michael, P. (2020). E-Government implementation challenges in small countries: The project manager's perspective. *Technological Forecasting and Social Change*, *152*, 119880.

Gosavi, A. (2018). Can mobile money help firms mitigate the problem of access to finance in Eastern sub-Saharan Africa? *Journal of African Business*, *19*(3), 343-360.

Hillman, S., & Neustaedter, C. (2017). Trust and mobile commerce in North America. *Computers in Human Behavior*, *70*, 10-21.

Humbani, M., & Wiese, M. (2018). A cashless society for all: Determining consumers' readiness to adopt mobile payment services. *Journal of African Business*, *19*(3), 409-429.

Jagtiani, J., & John, K. (2018). Fintech: the impact on consumers and regulatory responses. *Journal of Economics and Business*, *100*, 1-6.

Jakhiya, M., Bishnoi, M. M., & Purohit, H. (2020). Emergence and Growth of Mobile Money in Modern India: A Study on the Effect of Mobile Money. *2020 Advances in Science and Engineering Technology International Conferences (ASET)*, 1-10. IEEE.

Jibril, A. B., Kwarteng, M. A., Pilik, M., Botha, E., & Osakwe, C. N. (2020). Towards understanding the initial adoption of online retail stores in a low internet penetration context: An exploratory work in Ghana. *Sustainability*, *12*(3), 854.

Kaatz, C. (2020). Retail in my pocket–replicating and extending the construct of service quality into the mobile commerce context. *Journal of Retailing and Consumer Services*, *53*, 101983.

Kang, J. (2018). Mobile payment in Fintech environment: trends, security challenges, and services. *Human-centric Computing and Information sciences*, *8*(1), 1-16.

Khan, B. U. I., Olanrewaju, R. F., Baba, A. M., Langoo, A. A., & Assad, S. (2017). A compendious study of online payment systems: Past developments, present impact, and future considerations. *International Journal of Advanced Computer Science and Applications*, *8*(5), 256-271.

Khalilzadeh, J., Ozturk, A. B., & Bilgihan, A. (2017). Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry. *Computers in Human Behavior*, *70*, 460-474.

Kim, D., Park, K., Lee, D. J., & Ahn, Y. (2020). Predicting mobile trading system discontinuance: The role of attention. *Electronic Commerce Research and Applications*, *44*, 101008.

Korableva, O.N., Durand, T., Kalimullina, O. V., & Stepanova, I. (2019, January). Usability Testing of MOOC: Identifying User Interface Problems. *ICEIS*, *2*, 468-475.

Lakshmi, K. K., Gupta, H., & Ranjan, J. (2017, December). USSD – Architecture analysis, security threats, issues and enhancements. *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*, 798-802. IEEE.

Lee, W. H., Miou, C. S., Kuan, Y. F., Hsieh, T. L., & Chou, C. M. (2018). A peer-to-peer transaction authentication platform for mobile commerce with semi-offline architecture. *Electronic Commerce Research*, *18*(2), 413-431.

Lin, K. Y., Wang, Y. T., & Huang, T. K. (2020). Exploring the antecedents of mobile payment service usage: Perspectives based on cost-benefit theory, perceived value, and social influences. *Online Information Review*, *44*(1), 299-318.

Liu, Y., Wang, M., Huang, D., Huang, Q., Yang, H., & Li, Z. (2019). The impact of mobility, risk, and cost on the users' intention to adopt mobile payments. *Information Systems and e-Business Management*, *17*(2), 319-342.

Liu, W., Wang, X., & Peng, W. (2020). State of the art: Secure mobile payment. *IEEE Access*, *8*, 13898-13914.

Madden, G., Banerjee, A., Rappoport, P. N., & Suenaga, H. (2017). E-commerce transactions, the installed base of credit cards, and the potential mobile E-commerce adoption. *Applied Economics*, *49*(1), 21-32.

Madise, S. (2019). Developments in Mobile Technology and the Emergence of Mobile Money. In *The Regulation of Mobile Money* (pp. 63-110). Cham: Palgrave Macmillan.

Malaquias, R. F., & Silva, A. F. (2020). Understanding the use of mobile banking in rural areas of Brazil. *Technology in Society*, *62*, 101260.

Mallik, A., Tran, C., & Twagirumukiza, A. (2020, October). USSD Digital Wallet. *2020 Intermountain Engineering, Technology and Computing (IETC)*, 1-5. IEEE.

Mega, B. (2020). *Framework for improved security on usage of mobile money application based on iris biometric authentication method in Tanzania*. Doctoral dissertation. The University of Dodoma.

MeT. (2001). MeT overview white paper (Version 2.0) – The Met Initiative – Enabling mobile eCommerce [PDF]. http://www.mobiletransaction.org/pdf/White%20Paper_2.0.pdf

Mohamed, A., & Nor, M. (2021). Assessing the Effects of the Mobile Money Service on Small and Medium Sized Enterprises: Study on EVC-Plus Services in Somalia. *American Journal of Industrial and Business Management*, *11*, 499-514. https://doi.org/10.4236/ajibm.2021.115031.

Mullan, J., Bradley, L., & Loane, S. (2017). Bank adoption of mobile banking: stakeholder perspective. *International Journal of Bank Marketing*, *35*(7), 1154-1174.

Munoz-Leiva, F., Climent-Climent, S., & Liébana-Cabanillas, F. (2017). Determinants of intention to use the mobile banking apps: An extension of the classic TAM model. *Spanish Journal of Marketing-ESIC*, *21*(1), 25-38.

Nakibuuka, J., Semwanga, A. R., & Were, M. C. (2019). Implementation of USSD technology to improve quality of routinely reported health data in a resource-limited setting. In: *Health Informatics Vision: From Data via Information to Knowledge* (pp. 162-165). IOS Press.

National Communication Authority. (2021). NCA. https://nca.org.gh/

Otor, S. U., Akumba, B. O., Idikwu, J. S., & Achika, I. P. (2020). An Improved Security Model for Nigerian Unstructured Supplementary Services Data Mobile Banking Platform. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *6*(3), 974-987.

Pal, A., Herath, T., & Rao, H. R. (2020). Is the convenience worth the risk? An investigation of mobile payment usage. *Information Systems Frontiers*, 1-21.

Prakasha, K., Muniyal, B., & Acharya, V. (2019). Enhanced authentication and key exchange for end-to-end security in mobile commerce using wireless public key infrastructure. *Information Discovery and Delivery*, *48*(1), 14-22.

Putritama, A. (2019). The mobile payment fintech continuance usage intention in Indonesia. *Journal Economia*, *15*(2), 243-258.

Sarkar, S., & Khare, A. (2019). Influence of expectation confirmation, network externalities, and flow on use of mobile shopping apps. *International Journal of Human–Computer Interaction*, *35*(16), 1449-1460.

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management*, *45*, 44-55.

Shital and Prakash. (2015). An Overview of Real-Time Secure SMS Transmission. *International Journal of Advanced Research in Computer and Communication Engineering*, *4*(1), 177-179.

Sharma, S. K., & Sharma, M. (2019). Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation. *International Journal of Information Management*, *44*, 65-75. https://doi.org/10.1016/j.ijinfomgt.2018.09.013

Siau, K., Lim, E. P., & Shen, Z. (2003). Mobile commerce: Current states and future trends. *Advances in Mobile Commerce Technologies*, 1-17. IGI Global.

Sudin, S., Ahmad, R. B., & Idrus, S. Z. S. (2018). A model of virus infection dynamics in mobile personal area network. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(2-4), 197-201.

Talwar, S., Dhir, A., Khalil, A., Mohan, G., & Islam, A. N. (2020). Point of adoption and beyond. Initial trust and mobile-payment continuation intention. *Journal of Retailing and Consumer Services*, *55*, 102086.

Tiwari, P., Garg, V., Singhal, A., & Puri, N. (2020, January). Mobile banking a myth or misconception. *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 781-786. IEEE.

Tripathi, S. (2020). A study on adoption of digital payment through mobile payment application with reference to Gujarat State. *International Journal of Trend in Scientific Research and Development*, *4*(3), 1110-1115.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quart*, *36*(1), 157-178.

Verkijika, S. F., & Neneh, B. N. (2021). Standing up for or against: A text-mining study on the recommendation of mobile payment apps. *Journal of Retailing and Consumer Services*, *63*, 102743.

Wang, F., Yang, N., Shakeel, P. M., & Saravanan, V. (2021). Machine learning for mobile network payment security evaluation system. *Transactions on Emerging Telecommunications Technologies*, e4226.

Wang, Z., Zhao, Z., Min, G., Huang, X., Ni, Q., & Wang, R. (2018). User mobility aware task assignment for mobile edge computing. *Future Generation Computer Systems*, *85*, 1-8.

Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile banking: evolution and threats: malware threats and security solutions. *IEEE Consumer Electronics Magazine*, *8*(2), 56-60.

Yan, X. (2021). Towards a More Competitive Mobile Payment Industry: Standardization and Beyond. *Journal of Competition Law and Economics*, *17*(2), 405-436.

Yeboah-Asiamah, E., Nimako, S. G., Quaye, D. M., & Buame, S. (2016). Implicit and explicit loyalty: The role of satisfaction, trust and brand image in mobile telecommunication industry. *International Journal of Business and Emerging Markets*, *8*(1), 94-115.

Zhu, D. H., Lan, L. Y., & Chang, Y. P. (2017). Understanding the Intention to Continue Use of a Mobile Payment Provider: An Examination of Alipay Wallet in China. *International Journal of Business and Information*, *12*(4).
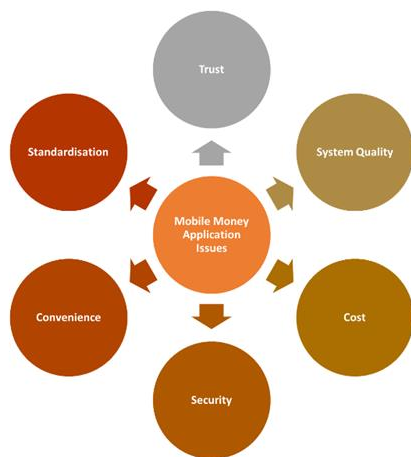
Appendix

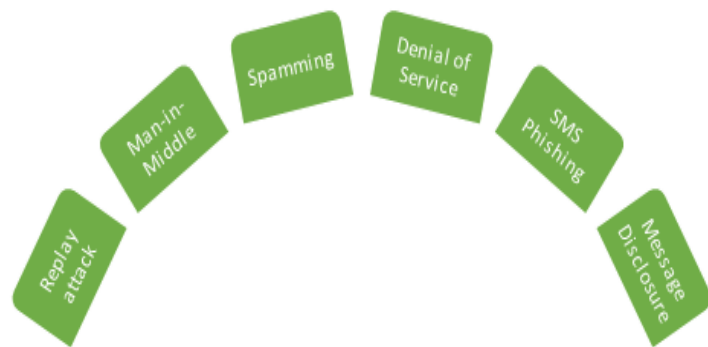Figure 1. Mobile money application issues

Figure 2. SMS threats

Figure 3. Length of PIN

Figure 4. Unmasked PIN

```
class Accounts(db.Model):
id = db.Column('account_id', db.Integer, primary_key=True)
name = db.Column(db.String(50))  # user input
phone = db.Column(db.String(15))  # user input or from ussd_session
email = db.Column(db.String(100))  # user input
pin = db.Column(db.String(6))  # user input
bank = db.Column(db.String(100)) #user input
account_number = db.Column(db.String(30)) #user input
bank_branch = db.Column(db.String(50)) #user input
balance = db.Column(db.String(200))  # default 0, user input (teller)
retry_chances = db.Column(db.Integer)  # default 3
creation_date = db.Column(db.String(10))  # progam generated
```
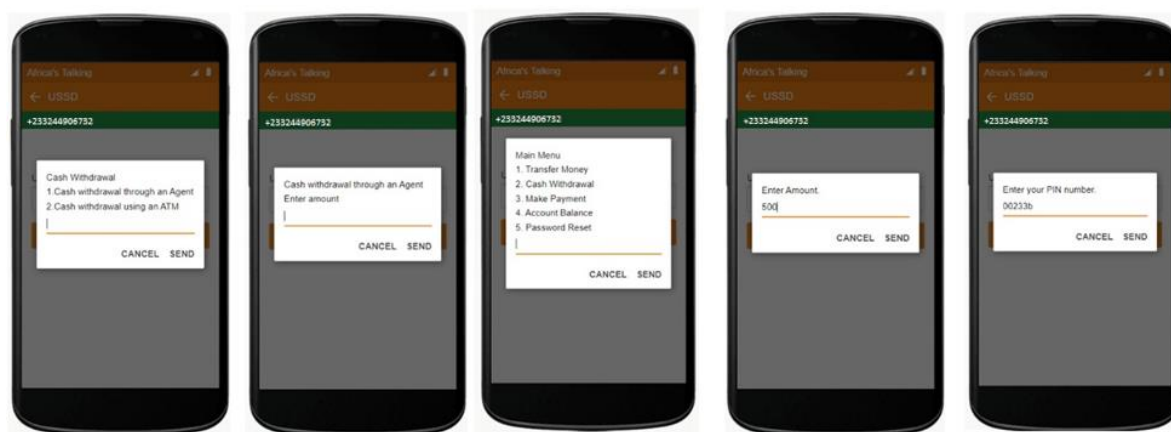
Figure 5. Programming code for User PIN keys

Figure 6. A summary of the user PIN of six characters

Table 1. Pattern of PIN used by users

Key M-Male F-Female	Digit of phone numbers		Year of birth		Others	
	15		23		19	
	F (9)	M(6)	F(15)	M(8)	F(6)	M(13)